JOURNAL OF ALGEBRA 47, 400–410 (1977)

On a Kaplansky Conjecture Concerning Three-Dimensional Division Algebras over a Finite Field*

GIAMPAOLO MENICHETTI

Mathematics Institute, University of Florence, Italy

Communicated by Guido Zappa

Received July 15, 1976

INTRODUCTION

The first important examples of three-dimensional division algebras over a finite field $K = GF(q)$, $q = p^h \geqslant 3$ and p prime, were presented by Dickson in [4]. Many authors since have studied other classes of such algebras. Particularly interesting, because not limited only to dimension three, is the class of twisted fields discovered by Albert [1] and generalized by the same author [3].

In [8], I determined the structure of any division algebra $\mathscr{A}$ with $\dim_K \mathscr{A} = 3$, indirectly making a classification of the whole set. In particular, under the hypothesis $q = p = 3m + 1$ which I examined in detail, I found that the number of nonassociative algebras $\mathscr{A}$ is $(p^3 - p^2 + p - 10)/3$.

Kaplansky [7] made the following conjecture: *Any three-dimensional division algebra over a finite field K is associative or a twisted field.* In the same paper the author determined the number of three-dimensional twisted fields over K showing it to be

$$\begin{aligned} \nu &= (q^3 - q^2 + q - 10)/3, \qquad \text{if} \quad q \equiv 1 \pmod 3, \\ \nu &= (q^3 - q^2 + q - 6)/3, \qquad \text{if} \quad q \not\equiv 1 \pmod 3. \end{aligned} \tag{1}$$

For $q = p = 3m + 1$, ν is also the number of all nonassociative algebras $\mathscr{A}$ determined in [8], thus proving the conjecture for this particular case. I am grateful to Kaplansky for this observation and for informing me of the content of [7] before its publication.

In Section 2 of this paper I prove Kaplansky's conjecture showing that, for any q, the number of all nonassociative three-dimensional division algebra over $K = GF(q)$ is given by (1). In Section 1 I give a short summary of the results proved in [8], which are needed in the next section.

* Work performed under the auspices of Italian Council of Research (C.N.R.).

ISSN 0021-8693

1. Let $K_3 = GF(q^3)$ be the field of rank 3 over $K = GF(q)$. Take an irreducible polynomial over $K[\xi]$,

$$f(\xi) = \sum_0^2{}_i e_i\xi^i - \xi^3, \qquad e_i \in K, \tag{2}$$

and fix one of its roots $v \in K_3 - K$.

For every $k = \sum_0^2{}_i x_i v^i \in K_3$, $x_i \in K$, let us consider the matrix

$$F(k) = \begin{pmatrix} x_0 & e_0x_2 & e_0x_1 + e_0e_2x_2 \\ x_1 & x_0 + e_1x_2 & e_1x_1 + (e_0 + e_1e_2)x_2 \\ x_2 & x_1 + e_2x_2 & x_0 + e_2x_1 + (e_1 + e_2{}^2)x_2 \end{pmatrix} = \sum_0^2{}_i x_iF^i, \tag{3}$$

where F is the element of $GL(3, K)$ given by

$$F = \begin{pmatrix} 0 & 0 & e_0 \\ 1 & 0 & e_1 \\ 0 & 1 & e_2 \end{pmatrix} = F(v).$$

Furthermore, let

$$\det(F(k) - tI) = \sum_0^2{}_i (-1)^i \sigma_{3-i}(F(k))t^i - t^3 \tag{4}$$

denote the characteristic polynomial of $F(k)$.

If

$$H = \begin{pmatrix} 1 & v & v^2 \\ 1 & v^q & v^{2q} \\ 1 & v^{q^2} & v^{2q^2} \end{pmatrix} \quad \text{and} \quad V = \begin{pmatrix} v & 0 & 0 \\ 0 & v^q & 0 \\ 0 & 0 & v^{q^2} \end{pmatrix},$$

then $F = H^{-1}VH$; therefore, $F(k) = H^{-1}V(k)H$, where

$$V(k) = \begin{pmatrix} k & 0 & 0 \\ 0 & k^q & 0 \\ 0 & 0 & k^{q^2} \end{pmatrix}.$$

For every $k \in K_3$, it follows that

$$\sum_0^2{}_i (-1)^i \sigma_{3-i}(F(k))k^i - k^3 = 0; \tag{5a}$$

$$\sigma_1(F(k^{q^s})) = \sigma_1(F(k)) = \sum_0^2{}_i k^{q^i}, \qquad s = 1, 2; \tag{5b}$$

$$\sigma_2(F(k^{q^s})) = \sigma_2(F(k)) = kk^q + kk^{q^2} + k^qk^{q^2}, \qquad s = 1, 2; \tag{5c}$$

$$\sigma_3(F(k^{q^s})) = \sigma_3(F(k)) = k^{1+q+q^2}, \qquad s = 1, 2. \tag{5d}$$

Moreover,

$$\sigma_1(F(k_1 + k_2)) = \sigma_1(F(k_1)) + \sigma_1(F(k_2)), \qquad \forall k_1, k_2 \in K_3; \tag{6a}$$

$$\sigma_1(F(k^2)) = \sigma_1{}^2(F(k)) - 2\sigma_2(F(k)), \qquad \forall k \in K_3; \tag{6b}$$

$$\sigma_1(F(ck)) = c\sigma_1(F(k)), \qquad \sigma_1(F(c)) = 3c, \qquad \forall k \in K_3 \text{ and } c \in K. \tag{6c}$$

In the rest of the paper

$$\text{l.i. } [k_1, k_2]_K \tag{7}$$

denotes that $1, k_1$, and

$$\varphi(k_1, k_2) = (k_1 + k_2)(\sigma_1(F(k_2)) - k_2) - \sigma_2(F(k_2)) \tag{8}$$

are elements of K_3 linearly independent over K.

In [8] it is proved that

$$\text{l.i. } [k_1, k_2]_K \Leftrightarrow \text{l.i. } [k_2, k_1]_K. \tag{9}$$

We denote by $\mathscr{A}_U(k_1, k_2)$ a three-dimensional algebra over K defined by the constants of multiplication, $c_{ij}^r = c_{ij}^r(k_1, k_2)$, relative to the chosen basis $U = \{u_0, u_1, u_2\}$. Assuming $u_i u_j = \sum_0^2 {}_r\, c_{ij}^r u_r$, $i, j = 1, 2, 3$, these constants are given by

$$\begin{gathered}
c_{0i}^r = c_{i0}^r = \delta_i{}^r, \qquad c_{11}^0 = c_{11}^1 = 0, \qquad c_{11}^2 = 1, \\
c_{12}^r = (-1)^r \sigma_{3-r}(F(k_1)), \qquad c_{21}^r = (-1)^r \sigma_{3-r}(F(k_2)), \\
c_{22}^0 = \sigma_1(F(k_1))\,\sigma_3(F(k_2)) + \sigma_1(F(k_2))\,\sigma_3(F(k_1)) - \sigma_2(F(k_1k_2)), \\
c_{22}^1 = -\sigma_3(F(k_1 + k_2)), \qquad c_{22}^2 = \sigma_1(F(k_1))\,\sigma_1(F(k_2)) - \sigma_1(F(k_1k_2)),
\end{gathered} \tag{10}$$

where k_1, k_2 are elements satisfying (7) and as usual

$$\delta_i{}^r = 1, \qquad \text{for } r = i,$$

$$\delta_i{}^r = 0, \qquad \text{for } r \neq i.$$

Propositions 1–4 are a synopsis of the results in [8].

PROPOSITION 1. *For every k_1, k_2 satisfying (7), $\mathscr{A} = \mathscr{A}_U(k_1, k_2)$ is a division algebra. In particular*:

(i) *$\mathscr{A}$ is associative iff $k_2 = k_1^{q^s}$, $s = 1, 2$.*

(ii) *$\mathscr{A}$ is commutative nonassociative iff $k_2 = k_1$ and $p \neq 2$.* ∎

Remark. By (10) we have $u_0u_i = u_iu_0 = u_i$, $\forall i \in \{0, 1, 2\}$. Hence u_0 is the unit of $\mathscr{A}$. Moreover, K is isomorphic to the subalgebra $\mathscr{A}' = \{xu_0 : x \in K\} \subset \mathscr{A}$.

In the rest of the paper $\mathscr{A}'$ is identified with K and 1 is written in place of u_0.

By (10) we have also $u_2 = u_1^2$; therefore, u_1 and u_2 are replaced by u and u^2, respectively. Hence $U = \{1, u, u^2\}$.

PROPOSITION 2. *Let $\mathscr{A} = \mathscr{A}_U(k_1, k_2)$ be a given nonassociative algebra, i.e., $k_2 \neq k_1^{q^s}$, $s = 1, 2$. Then:*

(i) *$U' = \{1, u', u'^2\}$ is a base of $\mathscr{A}$ for every $u' \in \mathscr{A} - K$.*

(ii) *If $u = \sum_0^2 \lambda_r u'^r$, $\lambda_r \in K$, then the constants of multiplication relative to the base U' are given by $c_{ij}^r(k_1', k_2')$, where*

$$\begin{aligned} k_1' &= \lambda_0 + \lambda_1 k_1^{q^i} + \lambda_2 \varphi^{q^i}(k_1, k_2) \\ k_2' &= \lambda_0 + \lambda_1 k_2^{q^i} + \lambda_2 \varphi^{q^i}(k_2, k_1) \end{aligned} \qquad i \in \{0, 1, 2\}. \tag{11}$$

Conversely, let k_1' and k_2' be given elements of the form (11), where $\lambda_j \in K$ and $(\lambda_1, \lambda_2) \neq (0, 0)$. Then there exists a base U' such that $c_{ij}^r(k_1', k_2')$ are the relative constants of multiplication. ∎

Remark. By (5) and (10) it follows that $c_{ij}^r(k_1', k_2') = c_{ij}^r(k_1'^{q^s}, k_2'^{q^s})$, $\forall i, j, r \in \{0, 1, 2\}$ and $s \in \{1, 2\}$.

PROPOSITION 3. *Any three-dimensional division algebra over K is isomorphic to an algebra $\mathscr{A}(k) = \mathscr{A}_U(v, k)$, where $k \in K_3$ is an element such that*

$$\text{l.i. } [v, k]_K. \quad ∎ \tag{12}$$

PROPOSITION 4. *Let $\mathscr{A}(k)$ be a nonassociative algebra, i.e., $k \neq v^{q^s}$, $s = 1, 2$. Then $\mathscr{A}(k')$ is isomorphic to $\mathscr{A}(k)$ iff there exists $i \in \{0, 1, 2\}$ and $\lambda_j \in K$ such that*

$$v = \lambda_0 + \lambda_1 v^{q^i} + \lambda_2 \varphi^{q^i}(v, k) \tag{13a}$$

and

$$k' = \lambda_0 + \lambda_1 k^{q^i} + \lambda_2 \varphi^{q^i}(k, v). \quad ∎ \tag{13b}$$

Remark. Let $k \neq v^{q^s}$, $s = 1, 2$, be a given element satisfying (12) and i be fixed in $\{0, 1, 2\}$. Then (13a) determines a unique triple $(\lambda_0, \lambda_1, \lambda_2) \in K^3$ and the corresponding element k' in (13b) satisfies (12). If $i = 0$, then $\lambda_0 = \lambda_2 = 0$, $\lambda_1 = 1$ and, so, $k' = k$. If $i \neq 0$, then either $k' = k$ or $k' \neq k$.

We examine these two possibilities in the following proposition.

PROPOSITION 5. *Let $k \neq v^{q^s}$, $s = 1, 2$, be a given element satisfying (12). Then the system*

$$\begin{aligned} v &= y_0 + y_1 v^{q^i} + y_2 \varphi^{q^i}(v, k) \\ k &= y_0 + y_1 k^{q^i} + y_2 \varphi^{q^i}(k, v) \end{aligned} \tag{14}$$

has one solution $(y_0, y_1, y_2) \in K^3$ either for every $i \in \{0, 1, 2\}$ or for $i = 0$ only.

Proof. Since $1, v, \varphi(v, k)$ are linearly independent over K, for every $i \in \{0, 1, 2\}$ there exists a unique triple $(y_{0i}, y_{1i}, y_{2i}) \in K^3$ such that

$$v = y_{0i} + y_{1i}v^{q^i} + y_{2i}\varphi^{q^i}(v, k). \tag{15}$$

In particular $(y_{00}, y_{10}, y_{20}) = (0, 1, 0)$.

Let

$$k_i = y_{0i} + y_{1i}k^{q^i} + y_{2i}\varphi^{q^i}(k, v), \qquad i = 0, 1, 2, \quad (k_0 = k) \tag{16}$$

and $\mathscr{A} = \mathscr{A}_U(v, k)$, $U = \{1, u, u^2\}$. By Proposition 2 it follows that if

$$u = \sum_0^2{}_r\, y_{ri}u_i^r, \qquad i = 0, 1, 2, \quad (u_0 = u) \tag{17}$$

then $c_{ij}^r(v, k_i)$ are the constants of multiplication of $\mathscr{A}$ relative to the basis $U_i = \{1, u_i, u_i^2\}$, $i = 0, 1, 2$.

The expressions (15) show that the triples (y_{0i}, y_{1i}, y_{2i}), $i = 0, 1, 2$, are distinct; hence the elements u_i, $i = 0, 1, 2$, also are distinct.

The conclusion follows from $k_1 = k \Leftrightarrow k_2 = k$, which we now prove.

Let $k_1 = k$. The constants of multiplication of $\mathscr{A} = \mathscr{A}_{U_1}(v, k)$, relative to the basis U_2, are $c_{ij}^r(v, k_2)$. Therefore according to Proposition 2, if

$$u_1 = \sum_0^2{}_r\, \lambda_r u_2^r, \tag{18}$$

then

$$v = \lambda_0 + \lambda_1 v^{q^i} + \lambda_2 \varphi^{q^i}(v, k) \tag{19a}$$

and

$$k_2 = \lambda_0 + \lambda_1 k^{q^i} + \lambda_2 \varphi^{q^i}(k, v), \tag{19b}$$

where $i \in \{0, 1, 2\}$.

From (15) and (19a) it follows that $(\lambda_0, \lambda_1, \lambda_2) = (y_{0i}, y_{1i}, y_{2i})$, $i \in \{0, 1, 2\}$. The cases $i = 0$ and $i = 2$ are impossible since (17) and (18) would then imply $u_1 = u_2$ and $u_1 = u_0$, respectively. Then necessarily $i = 1$ and $(\lambda_0, \lambda_1, \lambda_2) = (y_{01}, y_{11}, y_{21})$; so, from (16) and (19b) it follows that $k_2 = k_1\ (= k)$.

The proof of $k_2 = k \Rightarrow tk_1 = k$ is similar. ∎

2. By (9) it follows that (12) is equivalent to l.i. $[k, v]_K$. Therefore $k = \sum_0^2{}_i\, x_i v^i$ satisfies (12) iff

$$\begin{aligned} d(x_0, x_1, x_2) &= \det \begin{pmatrix} 1 & x_0 & e_1 + e_2x_0 - e_0x_2 \\ 0 & x_1 & e_2(x_1 + 1) - x_0 - e_1x_2 \\ 0 & x_2 & -(x_1 + 1) \end{pmatrix} \\ &= (x_0 + e_1x_2)x_2 - (x_1 + 1)(x_1 + e_2x_2) \neq 0. \end{aligned} \tag{20}$$

The equation $d(x_0, x_1, x_2) = 0$ has $(q+1)q$ solutions in K^3 because it represent a hyperbolic quadric of the three-dimensional affine space, $\mathbf{A}(3, q)$, over K. Then the order of

$$A = \{k \in K_3 : \text{l.i. } [v, k]_K,\ k \neq v^{q^s},\ s = 1, 2\} \tag{21}$$

is equal to $q^3 - q^2 - q - 2$.

According to Proposition 5 the set A can be decomposed into two disjoint classes, A_1 and A_2, where:

A_1 is the set of elements $k \in A$ for which the system (14) has one solution only when $i = 0$;

A_2 is the set of elements $k \in A$ for which the system (14) is solvable for any $i \in \{0, 1, 2\}$.

Let

$$|A_2| = n;$$

then

$$|A_1| = |A| - n = q^3 - q^2 - q - 2 - n.$$

From Propositions 3, 4, and 5 it follows that the number of all nonassociative three-dimensional division algebras over K is

$$\nu' = |A_1|/3 + |A_2| = (q^3 - q^2 - q - 2 + 2n)/3.$$

The proof that $\nu' = \nu$ (cf. (1)) follows after showing that

$$\begin{aligned} n &= q - 4, \quad \text{if } q \equiv 1 \pmod 3 \\ n &= q - 2, \quad \text{if } q \not\equiv 1 \pmod 3. \end{aligned} \tag{22}$$

To prove (22), it is convenient to assume in (2) that

$$e_2 = 0, \qquad e_1 \neq 0. \tag{23}$$

The existence, for any q, of polynomials $e_0 + e_1\xi - \xi^3$, $e_1 \neq 0$, irreducible over $K[\xi]$ follows from this remark:

Remark. If $p = 3$, then there is in $K[\xi]$ some irreducible polynomial $g_e(\xi) = e + \xi - \xi^3$. Indeed, $g_e(\xi_0) = 0 \Rightarrow g_e(\xi_0 + 1) = g_e(\xi_0 - 1) = 0$; also if $e' \neq e$ and $g_e(\xi_0) = 0$, $g_{e'}(\xi_0') = 0$, then $\xi_0' \neq \xi_0$. Therefore the q polynomials $g_e(\xi)$ cannot all be reducible.

If $p \neq 3$, then, with the substitution $\xi = \xi' + e_2/3$, from a given irreducible polynomial (2) a new irreducible polynomial $f'(\xi') = e_0' + e_1'\xi' - \xi'^3 \in K[\xi']$ is obtained.

In the particular case $e_1' = 0$ we can observe that $f''(\xi'') = e_0'(e_0' + 1) + 3e_0'\xi'' - \xi''^3$ is irreducible in $K[\xi'']$. Indeed, if ξ_0' is a root of $f'(\xi')$, i.e., $\xi_0'^3 = e_0'$,

then $\xi_0'' = \xi_0'^2 + \xi_0'$ is a root of $f''(\xi'')$. Moreover ξ_0'' belongs to $K_3 - K$; otherwise, $\xi_0' \in K_3 - K$ would be a root of the irreducible polynomial $\xi'^2 + \xi' - \xi_0'' \in K[\xi']$ and, hence, K_3 would contain the field of rank 2 over K.

LEMMA 1. *The linear system* (14) *has one solution in* K^3 *for every* $i \in \{0, 1, 2\}$ *iff*

$$\sigma_1(F(k)) = \sigma_1(F(v)) \ (= e_2 = 0) \tag{24a}$$

and

$$\sigma_2(F(k)) = \sigma_2(F(v)) \ (= -e_1). \tag{24b}$$

Proof. Necessity. Assume that (14) is solvable for every $i \in \{0, 1, 2\}$; that is,

$$\left.\begin{aligned} v^{q^i} &= y_{0i} + y_{1i}v + y_{2i}\varphi(v, k) \\ k^{q^i} &= y_{0i} + y_{1i}k + y_{2i}\varphi(k, v) \end{aligned}\right\}, \qquad i = 0, 1, 2,$$

with $y_{ji} \in K$ and $y_{00} = y_{20} = 0$, $y_{10} = 1$.

Replacing these expressions in $\sum_0^2{}_i v^{q^i} - \sigma_1(F(v)) = 0$ we find

$$\sum_0^2{}_i y_{0i} + v\sum_0^2{}_i y_{1i} + \varphi(v, k)\sum_0^2{}_i y_{2i} = 0;$$

hence, by (12),

$$\sum_0^2{}_i y_{0i} = \sum_0^2{}_i y_{1i} = \sum_0^2{}_i y_{2i} = 0.$$

In a similar way, from $\sum_0^2{}_i k^{q^i} - \sigma_1(F(k)) = 0$ and considering (9) and (12), we deduce

$$\sum_0^2{}_i y_{0i} - \sigma_1(F(k)) = \sum_0^2{}_i y_{1i} = \sum_0^2{}_i y_{2i} = 0.$$

Hence $\sigma_1(F(k)) = \sigma_1(F(v)) = 0$.

To prove (24b), we distinguish two cases.

(a) $y_{21} = 0$.

$$v^q = y_{01} + y_{11}v \Rightarrow v^{q^2} = y_{01} + y_{11}v^q = y_{01}(1 + y_{11}) + y_{11}^2 v^2$$

$$\Rightarrow vv^q + vv^{q^2} + v^q v^{q^2} =$$

$$y_{01}^2(1 + y_{11}) + 2y_{01}(1 + y_{11} + y_{11}^2)v + y_{11}(1 + y_{11} + y_{11}^2)v^2.$$

In particular, we have $\sigma_2(F(v)) = y_{01}^2(1 + y_{11})$ since $\{1, v, v^2\}$ is a basis of K_3.

Arguing analogously, we can prove that from $k^q = y_{01} + y_{11}k$, $\sigma_2(F(k)) = y_{01}^2(1 + y_{11})$ follows.

(b) $y_{21} \neq 0$.

By (5), (6), (8), and (24a), $v^q = y_{01} + y_{11}v + y_{21}\varphi(v, k) \Rightarrow \sigma_1(F(v^q)) = 0 = 3y_{01} + y_{21}\sigma_1(F(\varphi(v, k))) = 3y_{01} - y_{21}[\sigma_1(F(vk) + \sigma_1(F(k^2)) + 3\sigma_2(F(k))] = 3y_{01} - y_{21}[\sigma_1(F(vk)) + \sigma_2(F(k))] \Rightarrow \sigma_2(F(k)) = 3y_{01}y_{21}^{-1} - \sigma_1(F(vk))$.

In a similar way we can deduce $\sigma_2(F(v)) = 3y_{01}y_{21}^{-1} - \sigma_1(F(kv))$ from $k^q = y_{01} + y_{11}k + y_{21}\varphi(k, v)$.

Sufficiency. Assume that (24) hold and let

$$v^q = y_0 + y_1 v + y_2\varphi(v, k), \qquad y_j \in K, \tag{25a}$$

$$k^q = y_0' + y_1'k + y_2'\varphi(k, v), \qquad y_j' \in K. \tag{25b}$$

It suffices to show that $y_j' = y_j$, $j = 0, 1, 2$.

Raising the left and the right sides of (25a) to the power q^i, $i = 0, 1, 2$, we have

$$v^q = y_0 + y_1 v + y_2\varphi(v, k),$$

$$v^{q^2} = y_0 + y_1 v^q + y_2\varphi^q(v, k),$$

$$v = y_0 + y_1 v^{q^2} + y_2\varphi^{q^2}(v, k).$$

Using Cramer's rule and considering (5), (6), and (24) we find

$$y_j = C_j C^{-1}, \qquad j = 0, 1, 2,$$

where

$$\begin{aligned} C_0 &= \sigma_1(F(u^{q+1})) - \sigma_1(F(u^q(vk^q + v^q k))) + \sigma_1(F(u))\,\sigma_2(F(v)), \\ C_1 &= \sigma_1(F(u^q w - uw)),\ C_2 = 3\sigma_2(F(v)),\ C = \sigma_1(F(uw^q - u^q w)), \end{aligned} \tag{26}$$

and

$$u = vk, \qquad w = v + k.$$

After comparing (25b) with (25a) we can assert that the expressions of y_j' differ formally from the corresponding ones of y_j because of the exchange between v and k. Since u, w, and $\sigma_2(F(v))$ are invariant with respect to this exchange, it follows that (26) are also invariant. Hence $y_j' = y_j$, $j = 0, 1, 2$. ∎

From Lemma 1,

$$A_2 = \{k \in A: \sigma_1(F(k)) = 0, \sigma_2(F(k)) = -e_1\} \tag{27}$$

follows.

LEMMA 2. *Suppose $p \neq 3$. The polynomial*

$$l(\xi) = e_1^2\xi^2 + 9e_0\xi + 3e_1$$

is reducible in $K[\xi]$ iff $q \equiv 1 \pmod 3$. Also in this case, $l(\xi) = 0$ has two distinct roots in K.

Proof. Let $v^q = \sum_0^2 {}_i\, z_i v^i$ and, hence,

$$v^{q^2} = -v - v^q = -z_0 - (1 + z_1)v - z_2 v^2.$$

Since $\sigma_1(F(v^{q^s})) = 0$, $\sigma_2(F(v^{q^s})) = -e_1$, $s = 1, 2$, by (3) and (23) we obtain

$$\begin{aligned} 3z_0 + 2e_1 z_2 &= 0 \\ e_1(2z_1 + 1) + 3e_0 z_2 &= 0 \end{aligned} \tag{28a}$$

and

$$e_1^2 z_2^2 + 3e_1(z_1^2 - 1) + 9e_0 z_1 z_2 = 0. \tag{28b}$$

Solving (28a) with respect to z_0, $2z_1 + 1$, z_2, we find

$$z_0 = -2he_1^2, \qquad 2z_1 + 1 = -9he_0, \qquad z_2 = 3he_1,$$

where h is an element of K, which, according to (28b), we suppose also different from 0. Then

$$e_0 = -(2z_1 + 1)/9h, \qquad e_1 = z_2/3h, \qquad e_1^2 = (z_0 + e_1 z_2)/h. \tag{29}$$

After substituting these expressions into (28b), we obtain $(z_0 + e_1 z_2)z_2^2 + (z_1^2 - 1)z_2 - (2z_1 + 1)z_1 z_2 = 0$. Since (23) and (29) imply $z_2 \neq 0$, from this we have

$$(z_0 + e_1 z_2)z_2 = z_1^2 + z_1 + 1. \tag{30}$$

According to (29), the equation $l(\xi) = 0$ is equivalent to $(z_0 + e_1 z_2)\xi^2 - (2z_1 + 1)\xi + z_2 = 0$. From this, with the change of variable

$$\xi = (z_1 - \xi')(z_0 + e_1 z_2)^{-1} \tag{31}$$

and using (30), we find $l'(\xi') = \xi'^2 + \xi' + 1 = 0$.

Thus $l(\xi)$ is reducible over K iff $l'(\xi')$ is reducible; that is, iff the all cube roots of unity belong to K. It is known that, with $p \neq 3$, this occurs iff $q \equiv 1 \pmod 3$.

If $l'(\xi') = 0$ has two roots in K, then necessarily they are distinct; hence, from (31), those of $l(\xi) = 0$ are also distinct. ∎

PROPOSITION 6. *The order, n, of the set A_2 is given by* (22).

Proof. Let $k = \sum_0^2 {}_i\, x_i v^i$. According to (3), (20), and (23), we can write the conditions l.i. $[v, k]_K$, $\sigma_1(F(k)) = 0$, and $\sigma_2(F(k)) = -e_1$ in the following explicit form

$$\begin{aligned} (x_0 + e_1 x_2)x_2 - (x_1 + 1)x_1 &\neq 0 \\ 3x_0 + 2e_1 x_2 &= 0 \\ 3x_0^2 + 4e_1 x_0 x_2 - e_1 x_1^2 - 3e_0 x_1 x_2 + e_1^2 x_2^2 &= -e_1. \end{aligned} \tag{32}$$

We note that the above-mentioned conditions are also satisfied by $k = v^{q^s}$, $s = 1, 2$. Therefore, if n' is the number of solutions of the system (32), then, by (21) and (27),

$$| A_2 | = n = n' - 2. \tag{33}$$

We distinguish two cases.

(a) $p = 3$.

The system (32) becomes

$$x_1(x_1 + 1) \neq 0$$
$$x_2 = 0$$
$$x_1^2 = 1$$

and consequently has $n' = q$ solutions of the form $(x_0, 1, 0)$, $x_0 \in K$; so $n = q - 2$.

(b) $p \neq 3$.

In this case (32) is equivalent to the system

$$x_0 = -2e_1x_2/3$$
$$3e_1x_1^2 + 9e_0x_1x_2 + e_1^2x_2^2 = 3e_1$$
$$e_1x_2^2 - 3x_1(x_1 + 1) \neq 0.$$

Therefore n' is equal to the number of points of the affine plane $\mathbf{A}(2, q)$, over K, belonging to conic γ: $3e_1x_1^2 + 9e_0x_1x_2 + e_1^2x_2^2 - 3e_1 = 0$ but not to conic γ': $e_1x_2^2 - 3x_1(x_2 + 1) = 0$.

Since the point $P(-1, 0)$ belongs to each one of γ and γ', we determine a parametrization setting $x_2 = m(x_1 + 1)$. In this way we find

$$x_1 = (3e_1 - e_1^2m^2)(e_1^2m^2 + 9e_0m + 3e_1)^{-1} \tag{34}$$

and

$$x_1 = e_1m^2(3 - e_1m^2)^{-1} \tag{35}$$

for γ and γ', respectively.

From (34) we deduce that γ is irreducible. Indeed $3e_1 - e_1^2m^2 = 0$ and $e_1^2m^2 + 9e_0m + 3e_1 = 0$ iff $27e_0^2 - 4e_1^3 = 0$. But the last equality is impossible if $p = 2$ since $e_0 \neq 0$ and also if $p \neq 2$ since, from Lemma 2, the discriminant $3(27e_0^2 - 4e_1^3)$ of $l(\xi) = 0$ is different from 0.

Thus, in $\mathbf{A}(2, q)$, the number of points of γ is $q + 1$ minus the number of solutions of $l(m) = e_1^2m^2 + 9e_0m + 3e_1 = 0$ in K.

It is easy to prove that the values of x_1 given by (34) and (35) coincide iff $e_0m^3 + e_1m^2 - 1 = 0$, i.e., $f(1/m) = 0$. It follows that $P(-1, 0)$ is the only point of $\mathbf{A}(2, q)$ belonging to γ and γ'.

From above results and from Lemma 2, it follows that

$$n' = q - 2, \qquad \text{if} \quad q \equiv 1 \pmod 3$$
$$n = q, \qquad \text{if} \quad q \not\equiv 1 \pmod 3.$$

From this and from (33) we find (22). ∎

References

1. A. A. Albert, On nonassociative division algebras, *Trans. Amer. Math. Soc.* **72** (1952), 296–309.
2. A. A. Albert, Finite noncommutative division algebras, *Proc. Amer. Math. Soc.* **9** (1958), 928–932.
3. A. A. Albert, Generalized twisted fields, *Pacific J. Math.* **11** (1961), 1–8.
4. L. E. Dickson, On finite algebras, *Nachr. Ges. Wiss. Göttingen* (1905), 358–393.
5. L. E. Dickson, Linear algebras in which division is always uniquely possible, *Trans. Amer. Math. Soc.* **7** (1906), 370–390.
6. I. Kaplansky, Three-dimensional division algebras. I. *J. Algebra* **40** (1976), 384–391.
7. I. Kaplansky, Three-dimensional division algebras. II. *Houston Journal of Mathematics* **1** (1975), 63–79.
8. G. Menichetti, Algebre tridimensionali su un campo di Galois, *Ann. Mat. Pura Appl.* **97** (4) (1973), 283–302.